REMARKS

This Amendment is in response to the Office Action dated July 6, 2007 ("OA"). In the Office Action, claim 13 was objected to, claims 1-6, 13-16, 22 and 23 were rejected under 35 USC §101, claims 7-9 were rejected under 35 USC §102 and claims 1-6 and 10-23 were rejected under 35 USC §103. Claims 1-25 are believed allowable, with claims 1, 5, 7, 13, 17, 19, 22 and 23 being independent claims.

NEW CLAIMS:

Claim 24

Claim 24 is dependent on claim 7 and recites, "The hard disk device according to claim 7, wherein the control mechanism writes the data in the recording medium without encrypting the data when the encryption function is turned off."

Support for claim 24 is found in at least paragraph [0060] of the specification, which recites:

> The encryption circuit 54 encrypts the data and decrypts the encrypted data by use of an encryption algorithm. The selector 55 selects as to whether or not the write data or the read data are subjected to processing by the encryption circuit 54. App., para. [0060].

It is noted that the following passage of Jackson teaches *away* from writing data without encrypting the data when an encryption function is turned off:

> Preferably, the encryption/decryption means is formed and arranged such that, in its deactivated state, no data can pass therethrough. Consequently, where the permanent security control means is adapted to route all data to be written to, or read from, the disk(s) through the encryption/decryption means, if the encryption/decryption means is in its deactivated state no data can be written to or read from the disk(s), whether in encrypted form or otherwise. Jackson, para. [0015].

Claim 25

Claim 25 is dependent on claim 17 and recites, "The data processing method of claim 17, wherein the user verification comprises: creating a candidate encryption key out of a given piece of candidate

personal identification information; creating candidate verification data by encrypting the candidate personal identification information by use of the candidate encryption key; and determining whether the candidate verification data are identical to the verification data previously recorded in the recording medium."

Support for claim 25 is found in at least paragraph [0096] of the specification, which recites:

> As shown in FIG. 8, the personal identification information is firstly encrypted by the encryption circuit 54, whereby the verification encryption key is created (2-e). Then, the personal identification information is encrypted again by use of this verification encryption key, and the verification data are created (6-f). When the created verification data are identical to the verification data recorded in the magnetic disk 10, the verification succeeds in the verification processing by the CPU 58 and the hard disk device 100 is thereby activated (6-g). Moreover, the encrypted data encryption key is read out of the magnetic disk 10 and is decrypted with the encryption circuit 54 by use of the verification encryption key (6-h). Then, either encryption of the data to be transmitted from the computer device 200 and to be written in the magnetic disk 10, or decryption of the data read out of the magnetic disk 10 and to be transmitted to the computer device 200 is executed by the encryption circuit 54 using the data encryption key (6-i). App., para. [0096].

In rejecting claim 17, the Examiner alleged that paragraphs [0145] and [0150] of Matsuzaki teach executing user verification based on the verification data recorded in the recording medium. OA, pg. 7-8. Paragraph [0145] of Matsuzaki states:

> The decryption unit 205b reads the encrypted password stored in the storage unit 400b, and reads the key information from the key storage medium 20. The decryption unit 205b then subjects the read encrypted password to the decryption algorithm D1 using the read key information to generate a password, and outputs the generated password to the encryption unit 202b. Matsuzaki, para. [0145].

The Applicants respectfully submit that the cited passage fails to teach or suggest the limitations required by claim 25.

Furthermore, paragraph [0150] of Matsuzaki states:

> The encryption unit 202b receives the password from the

> decryption unit 205b and the file key from the file key generation unit 201b. The encryption unit 202b then subjects the received file key to the encryption algorithm E2 using the received password as a key to generate a first encrypted file key, and writes the generated first encrypted file key to the header part of the encrypted file 404b in the storage unit 400b. Matsuzaki, para. [0150].

The Applicants respectfully submit that the cited passage fails to teach or suggest the limitations required by claim 25.

Moreover, the Examiner alleges that "the encrypted password is decrypted and used as an encryption key to encrypt a file key." OA, pg. 7-8. The Applicants respectfully submit that decrypting an encrypted password and using the result as an encryption key to encrypt a file key is clearly not equivalent to the limitations introduced by claim 25.

CLAIM OBJECTIONS:

Claim 13

Claim 13 was objected to due to an informality regarding the language, "an verification key". OA, pg. 2. The Examiner suggested changing this language to "a verification key". *Id.* Claim 13 has been amended in the manner suggested by the Examiner. The Applicants thank the Examiner for pointing out this typographical error.

CLAIM REJECTIONS UNDER 35 USC §101:

Claims 1, 5, 13, 22 and 23 were rejected under 35 USC §101 as allegedly directed to non-statutory subject matter. The Office Action alleges claims 1, 5, 13, 22 and 23 "are rejected as being directed to functional descriptive material (i.e., computer software)." OA, pg. 2. The Applicants respectfully disagree with the Examiner.

35 U.S.C. § 101 provides:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1, 5 and 13 recite physical structures and not merely computer software, as alleged in the Office Action. For example, claims 1 and 5 recite data storage devices comprising, in part, an encryption circuit and a recording medium. Claim 13 an information

processing device including a data storage device. Thus, the Applicants respectfully submit that claims 1, 5 and 13 are not directed to functional descriptive material (software).

Moreover, there is no prohibition in patent laws against claiming computer software. "When a computer program is recited in conjunction with a physical structure, such as a computer memory, USPTO personnel should treat the claim as a product claim." *Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility*, pp. 53-54 (Oct. 26, 2005) (http://www.uspto.gov/web/offices/pac/dapp/opla/preognotice/guidelines101_20051026.pdf).

Claims 22 and 23 are amended herein to recite, in part, "A program stored in computer readable memory." Thus, claims 22 and 23 provide for a computer program in conjunction with a physical structure, namely a computer readable memory. Furthermore, the claims are directed to statutory subject matter and are believed to overcome the rejections under 35 USC §101.

Claims 2-4, 6 and 14-16 are dependent on and further limit claims 1, 5 and 13. Since claims 1, 5 and 13 are believed to be directed to statutory subject matter, claims 2-4, 6 and 14-16 are likewise believed to be directed to statutory subject matter.For at least these reasons, the Applicants respectfully submit that claims 1-6, 13-16, 22 and 23 are allowable and earnestly solicit allowance of the claims.

CLAIM REJECTIONS UNDER 35 USC §102:

Claims 7-9 were rejected under 35 USC §102 as being anticipated by European Patent Publication No. 0911738A2 ("Jackson"). OA, pg. 3.

Anticipation is established only when a single prior art reference discloses, expressly or under principles of inherency, each and every element of a claimed invention. RCA Corp. v. Applied Digital Data Sys., Inc., 730 F.2d 1440, 1444, 221 USPQ 385, 388 (Fed. Cir. 1984). In other words, there must be no difference between the claimed invention and the reference disclosure, as viewed by a person of ordinary skill in the field of the invention. Scripps Clinic & Research Found. v. Genentech Inc., 927 F.2d 1565, 1576, 18 USPQ2d 1001, 1010 (Fed. Cir. 1991).

Claim 7

Claim 7 recites, in part, "wherein the encryption function of the control mechanism encrypts personal identification information by use of an encryption key created out of a given piece of the personal identification information." Thus, claim 7 requires encrypting personal identification information by use of an encryption key. Furthermore, it is evident from antecedent basis that the personal identification information which is encrypted is the same personal identification information of which a given piece was used to create the encryption key.

The limitation requiring encrypting personal identification information by use of an encryption key created out of a given piece of the personal identification information was originally introduced in claims 10 and 12. Therefore, in responding to claim 7, the Applicants shall respond to the relevant arguments raised by the Examiner in regards to claims 10 and 12.

The Examiner concedes, "Jackson is silent on the device wherein the encryption key is created out of a given piece of the personal identification information." OA, pg. 13. However, the Examiner alleges that column 10, lines 48-65 of Johnson teaches creating an encryption key out of a given piece of personal identification information. OA, pg. 13. The cited passage states:

> The step 804 of initializing the UAS 12 with recognition and comprehension data is shown in greater detail in FIG. 4b. As shown in FIG. 4b, processor 30 starts the data initialization process by prompting 810 the user for a dynamic personal identification number (DPIN) or code. This DPIN may be any desired alpha-numeric which the user wants to use as an identification code. Step 810 is preferably carried out by sending a user prompt to the display subsystem 50 and soliciting a response from the user via the keyboard subsystem 52. Once a DPIN is received from the keyboard subsystem 52, processor 30 proceeds to generate 814 a master hash code and a master key code using the DPIN as input. As will be explained later, this master key code is used to encrypt information stored on the master EKE 70. Preferably, processor 30 generates the master key code in two steps. First, processor 30 executes the hash code generation logic stored in section 62 of the non-volatile memory 38, using the DPIN as input, to generate a master hash code. Processor 30 preferably generates the master hash code by implementing a hashing algorithm. In the preferred embodiment . . . . Johnson, col. 10, ln. 46-66.

The Applicants submit that column 10, lines 48-65 of Johnson do not disclose encrypting personal identification information and creating an encryption key out of a piece of the personal identification information. As previously noted, claim 7 requires that the personal identification information which is encrypted is the same as the personal identification information of which a given piece was used to create the encryption key.

For at least these reasons, the Applicants respectfully submit that claim 7 is not anticipated by Jackson. The Applicants further respectfully submit that claim 7 is not obvious over Jackson in view of Johnson. Accordingly, the Applicants earnestly solicit allowance of the claim.

Claim 8

Claim 8 is dependent on claim 7 and recites, "The hard disk device according to claim 7, wherein the control mechanism judges as to whether the data are encrypted or not upon reading the data out of the storage medium, and further decrypts the data when the data are encrypted." It is emphasized that claim 8 requires judging as to whether data are encrypted or not.

The Examiner alleges that pg. 11, para. 0041-0042 of Jackson teaches the limitation introduced by claim 8. OA, pg. 4. The passage cited by the Examiner recites:

> On a host read operation to read a file, the sequencer 2 will retrieve the encrypted file data from the disks 11 (via the VCM, spindle 9, motor 14 and read/write heads 13) and load it into the SRAM 1. From the SRAM the data is transferred in eight byte packets to the DED where it is decrypted. The plain text is then transferred back to the SRAM and is transferred to the host when the SRAM is full. Space is then made available in the SRAM. This process continues until the whole file has been read.
>
> On a host write operation, the plain text is transferred from the host to the SRAM 1 via the host interface 10 and sequencer 2. The data in the SRAM is transferred in eight byte packets to the DED 4 where it is encrypted. Once all the data in the SRAM has been encrypted, the sequencer 2 will transfer the cipher text from the SRAM to the disks 11. Space is made available in the SRAM. If more host data is available, it is transferred to the SRAM and the process is repeated. Jackson, para. 0041-0042.

The Applicants respectfully submit that the cited passage fails to teach or suggest judging as to whether data are encrypted or not as is required by claim 8.

For at least these reasons, the Applicants respectfully submit that claim 8 is not anticipated by Jackson and earnestly solicit allowance of the claim.

Claim 9

Claim 9 is dependent on and further limits claim 7. Since claim 7 is believed allowable, claim 9 is also believed allowable for at least the same reasons as claim 7.

CLAIM REJECTIONS UNDER 35 USC §103:

Claims 1, 2, 5, 6 and 13-23 were rejected under 35 USC §103 as unpatentable over U.S. Patent Application Publication No. 2001/0056541 ("Matsuzaki") in view of U.S. Patent No. 5,604,800 issued to Johnson et al. ("Johnson"). OA, pg. 4.

Claim 3 was rejected under 35 USC §103 as unpatentable over Matsuzaki in view of Johnson and further in view of U.S. Patent No. 7,062,652 issued to Hirota et al. ("Hirota"). OA, pg. 11.

Claim 4 was rejected under 35 USC §103 as unpatentable over Matsuzaki in view of Johnson and further in view of Jackson. OA, pg. 11.

Claims 10-12 were rejected under 35 USC §103 as unpatentable over Jackson in view of Johnson. OA, pg. 12.

A *prima facie* case for obviousness can only be made if the combined reference documents teach or suggest all the claim limitations. MPEP 2143. Furthermore, to establish a *prima facie* case of obviousness, there must be some suggestion or motivation to modify the reference or to combine reference teachings. MPEP 2143. It is well settled that "rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." In re Kahn, 441 F.3d 977, 988, 78 USPQ2d

1329, 1336, quoted with approval in KSR Int'l Co. v. Teleflex Inc., 127 S. Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007).

Claim 1

Claim 1 recites, in part, "an encryption circuit for encrypting desired data and personal identification information by use of an encryption key created out of a given piece of the personal identification information." Thus, claim 1 requires encrypting personal identification information by use of an encryption key. Furthermore, it is evident from antecedent basis that the personal identification information which is encrypted is the same personal identification information of which a given piece was used to create the encryption key.

The Examiner alleges that paragraphs [0141] and [0152] of Matzusaki teach an encryption circuit for encrypting desired data and personal identification information by use of an encryption key. OA, pg. 5. After careful review of Matzusaki, the Applicants respectfully disagree with this interpretation.

The paragraph [0141] of Matzusaki states:

> The encryption unit 102b, as the encryption unit 102, reads key information from the key storage medium 20, subjects the password received from the password input unit 101b to the encryption algorithm E1 using the read key information to generate an encrypted password, and writes the generated encrypted password as a file, to the storage unit 400b. Matsuzaki, para. [0141].

It is clear from this passage that the key information from the key storage medium and the password received from the password input unit are used to generate an encrypted password. By contrast, claim 1 requires encrypting personal identification information by use of an encryption key created out of a given piece of the personal identification information. Paragraph [0141] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The paragraph [0152] of Matzusaki states:

> The encryption unit 204b reads the key information from the key storage medium 20, receives the file key from the file key generation unit 201b. The encryption unit 204b then subjects the file key to the encryption algorithm E4 using the read key information as a key to generate a second encrypted file key, and

> writes the generated second encrypted file key to the header part of the encrypted file 404b in the storage unit 400b. It should be noted here that the encryption algorithm E4 complies with DES. Matsuzaki, para. [0152].

The Applicants respectfully submit that paragraph [0152] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The Examiner further alleges that column 10, lines 48-65 of Johnson teaches creating an encryption key out of a given piece of personal identification information. OA, pg. 5. The cited passage states:

> The step 804 of initializing the UAS 12 with recognition and comprehension data is shown in greater detail in FIG. 4b. As shown in FIG. 4b, processor 30 starts the data initialization process by prompting 810 the user for a dynamic personal identification number (DPIN) or code. This DPIN may be any desired alpha-numeric which the user wants to use as an identification code. Step 810 is preferably carried out by sending a user prompt to the display subsystem 50 and soliciting a response from the user via the keyboard subsystem 52. Once a DPIN is received from the keyboard subsystem 52, processor 30 proceeds to generate 814 a master hash code and a master key code using the DPIN as input. As will be explained later, this master key code is used to encrypt information stored on the master EKE 70. Preferably, processor 30 generates the master key code in two steps. First, processor 30 executes the hash code generation logic stored in section 62 of the non-volatile memory 38, using the DPIN as input, to generate a master hash code. Processor 30 preferably generates the master hash code by implementing a hashing algorithm. In the preferred embodiment . . . . Johnson, col. 10, ln. 46-66.

The Applicants submit that column 10, lines 48-65 of Johnson do not disclose encrypting personal identification information and creating an encryption key out of a piece of the personal identification information. As previously noted, claim 1 requires that the personal identification information which is encrypted is the same as the personal identification information of which a given piece was used to create the encryption key.

Additionally, the Examiner argues, "It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system." OA, pg. 5.

The Office Action, however has not explained, and it not evident, how employing the teachings of Johnson within the system of Matsuzaki enhances the security of the system. The Office Action has also not explained why a person of ordinary skill in the art would have found it obvious to reconstruct Matsuzaki to "enhance the security of the system." In this regard, neither Matsuzaki nor Johnson express any appreciation of such alleged advantages.

For at least these reasons, the Applicants respectfully submit that claim 1 is not obvious over Matsuzaki in view of Johnson and earnestly solicit allowance of the claim.

Claim 2

Claim 2 is dependent on claim 1 and recites, "The data storage device according to claim 1, wherein the encryption circuit encrypts the encryption key by use of a different encryption key, and the recording medium records the encryption key encrypted by use of the different encryption key." It is evident from antecedent basis that the encryption key recited in claim 2 is the same encryption key that was recited in claim 1.

The Examiner alleges that paragraphs [0148] through [0152] of Matsuzaki teach the limitations introduced by claim 2. OA, pg. 9. The passage cited by the Examiner states:

> The encryption unit 203b then subjects a plaintext included in the plaintext file 401b to the encryption algorithm E3 using the received file key as a key to generate a ciphertext, and writes an encrypted file 404b including the generated ciphertext in the data part thereof, to the storage unit 400.
>
> (7) Encryption Unit 202b
>
> The encryption unit 202b receives the password from the decryption unit 205b and the file key from the file key generation unit 201b. The encryption unit 202b then subjects the received file key to the encryption algorithm E2 using the received password as a key to generate a first encrypted file key, and writes the generated first encrypted file key to the header part of the encrypted file 404b in the storage unit 400b.
>
> (8) Encryption Unit 204b
>
> The encryption unit 204b reads the key information from the key storage medium 20, receives the file key from the file key generation unit 201b. The encryption unit 204b then subjects the file key to the encryption algorithm E4 using the read key information as a key to generate a second encrypted file key, and

> writes the generated second encrypted file key to the header part of the encrypted file 404b in the storage unit 400b. It should be noted here that the encryption algorithm E4 complies with DES. Matsuzaki, para. [0148]-[0152].

In regards to claim 1, the Examiner alleges that "encrypting file key using read key" teaches encrypting desired data by use of an encryption key as required by claim 1. OA, pg. 5. The Applicants interpret "read key" to refer to the read key information from the key storage medium, as the language "read key" is not used in any other context in paragraphs [0148] through [0152] of Matsuzaki. It follows from this statement that the Examiner is alleging the read key of Matsuzaki to be equivalent to the encryption key of claim 1.

As noted above, the encryption key of claim 2 is the same as the encryption key of claim 1. Therefore, Matsuzaki cannot teach claim 2 unless the read key information of Matsuzaki is equivalent to the encryption key of claim 2. It follows that Matsuzaki, alone or in combination with other teachings, cannot teach claim 2 unless the read key information is encrypted by use of a different encryption key.

The Applicants respectfully submit that the cited passage of Matsuzaki fails to teach or suggest encrypting the read key information by use of a different encryption key. The passage teaches that a plaintext and a file key are encrypted. However, this fails to teach or suggest claim 2 because the plaintext and the file key are clearly not equivalent to the read key information.

For at least these reasons, the Applicants respectfully submit that claim 2 is not obvious over Matsuzaki in view of Johnson and earnestly solicit allowance of the claim.

Claim 3

Claim 3 is dependent on claim 1 and recites, "The data storage device according to claim 1, wherein the recording medium includes a special storage area which is inaccessible in normal use, and the recording medium records the encryption key in the special storage area."

In rejecting claim 3, the Examiner alleges that "Hirota teaches a recording medium includes a special storage area which is inaccessible in normal use, and the recording medium records the encryption key in

the special storage area [see for example, column 12, lines 49-54 and column 10, lines 22-36]." OA, pg. 11.

The Examiner argues that the cited claim elements are found in Hirota by merely copying the claim elements and citing column and line numbers of Hirota in brackets. The rejection does not provide a comprehensive explanation of why the Examiner considers the limitations of claim 3 disclosed in Hirota. The Applicants are left guessing what the Examiner was thinking when making the rejection. If the rejection of claim 3 is maintained, the Applicants request that a detailed explanation of disclosed structures relied upon in Hirota be clearly articulated by the examiner in accordance with 37 CFR 1.104(c)(2).

The first passage cited by the Examiner states:

> The authentication area 332 stores an encryption key 425 which is a secret key used for decrypting the encrypted content 426 stored in the non-authentication area 331. The special area 304 stores the medium ID 341 which is necessary for accessing the authentication area 332. Hirota, col. 12, ln. 49-54.

The passage discloses an authentication area which stores an encryption key. However, absent from the cited passage is any teaching or suggestion that the authentication area is inaccessible in normal use.

The passage further discloses a special area which stores a medium ID. However, absent from the cited passage is any teaching or suggestion that the medium ID is equivalent to an encryption key.

The second passage cited by the Examiner states:

> The flash memory 303 is a flash-erasable, rewritable nonvolatile memory of a block deletion type, and includes logical storage areas: an authentication area 332 and a non-authentication area 331. The authentication area 332 can be accessed only by the apparatuses that have been authenticated as proper apparatuses. The non-authentication area 331 can be accessed by any apparatuses whether they are authenticated or not. In the present embodiment, the authentication area 332 is used for storing important data related to copyright protection, and the non-authentication area 331 is used as an auxiliary storage apparatus in a typical computer system. Note that a certain address in the flash memory 303 is used as a boundary between these two storage areas. Hirota, col. 10, ln. 22-36.

The cited passage discloses that the authentication area can be accessed only by apparatuses that have been authenticated as proper apparatuses. The Applicants respectfully submit that a storage area which can be accessed only by apparatuses that have been authenticated as proper apparatuses is not inherently equivalent to a storage area which is inaccessible in normal use. In particular, the accesses by "proper apparatuses" may constitute normal use.

Additional information about the authentication area (num. 332) disclosed by Hirota is disclosed in the following passage:

> It is therefore an object of the present invention to provide a semiconductor memory card that can be used as a storage medium for storing digital contents and as a storage medium for storing general-purpose computer data (not an object of copyright protection), and to provide an apparatus for reading data from the storage medium.
>
> The above object is fulfilled by a semiconductor memory card that can be used/removed in/from an electronic device, comprising: a rewritable nonvolatile memory; and a control circuit which controls accesses by the electronic device to an authentication area and a non-authentication area in the rewritable nonvolatile memory, wherein the control circuit includes: a non-authentication area access control unit which controls accesses by the electronic device to the non-authentication area; an authentication unit which performs an authentication process to check whether the electronic device is proper, and affirmatively authenticates the electronic device when the electronic device is proper; and an authentication area access control unit which permits the electronic device to access the authentication area only when the authentication unit affirmatively authenticates the electronic device.
>
> With the above construction, the data being an object of copyright protection can be stored in the authentication area and other data can be stored in the non-authentication area, which makes it possible to achieve a semiconductor memory card which is capable of storing both digital contents to be copyright-protected and other data together. Hirota, col. 2, ln. 6-33.

The cited passage discloses that data being an object of copyright protection are stored in the authentication area disclosed in Hirota. Furthermore, the passage clearly states, "It is therefore an object of the present invention to provide . . . a storage medium for storing digital contents . . . ." Hirota, col. 2, ln. 6-8. It is thus evident that accessing the data being an object of copyright protection is central to the invention of Hirota. This suggests that accessing this data occurs during normal use. Because this data is stored in the

authentication area, it follows that the authentication area disclosed by Hirota is accessed in normal use. The Applicants respectfully submit that because claim 3 requires the special storage area to be inaccessible in normal use, the authentication area of Hirota cannot be equivalent to the special storage area of claim 3.

For at least these reasons, the Applicants respectfully submit that claim 3 is not obvious over Matsuzaki in view of Johnson and further in view of Hirota and earnestly solicit allowance of the claim.

Claim 4

Claim 4 is dependent on claim 1 and recites, "The data storage device according to claim 1, wherein the encryption circuit creates a plurality of encryption keys out of a plurality of personal identification information and controls the user identification and the data encryption depending on each of the plurality of encryption keys, and the recording medium manages the storage areas in accordance with the plurality of keys, and records the encrypted data in the respective storage areas by use of the corresponding encryption keys." It is emphasized that claim 4 requires the plurality of encryption keys to be created out of a plurality of personal identification information. Moreover, it is emphasized that claim 4 requires controlling user identification depending on each of the plurality of encryption keys.

The Examiner alleges that col. 8, ln. 33-47 of Jackson teach claim 4. OA, pg. 12. The Examiner argues that the cited claim elements are found in Jackson by merely copying the claim elements and citing column and line numbers of Jackson in brackets. The rejection does not provide a comprehensive explanation of why the Examiner considers the limitations of claim 4 disclosed in Jackson. The Applicants are left guessing what the Examiner was thinking when making the rejection. If the rejection of claim 4 is maintained, the Applicants request that a detailed explanation of disclosed structures relied upon in Jackson be clearly articulated by the examiner in accordance with 37 CFR 1.104(c)(2).

The passages cited by the Examiner recite:

> CBC (and pipeline mode) require both a CV and an IV to be loaded in order to enable the drive. The IV would be a string of characters unique to the particular drive, perhaps including the

> serial number. The process is similar to that just described but an additional level of security is provided. In this case, the encryption algorithm for each sector of data will be based on the internal CV and an internal IV unique to the drive and that sector. This internal IV would be typically based on the input IV (itself depending on the drive serial number, for example) and on the logical block address of the sector in question. An advantage of this approach arises when identical data is written to each sector since the resulting encrypted data will differ sector by sector, making it more difficult to decode the encrypted data. Jackson, col. 8, ln. 33-47.

The Applicants respectfully submit that the cited passage fails to teach or suggest a plurality of encryption keys which is created out of a plurality of personal identification information as required by claim 4. The cited passage discloses a plurality of IV's. However, the passage fails to teach or suggest that the plurality of IV's are created out of a plurality of personal identification information. To the contrary, the passage teaches that the internal IV's (e.g., those specific to a sector) are calculated based on the logical block address of the sector with which the internal IV is associated and on an "input IV" which may depend on the drive serial number. It is evident that logical block addresses and drive serial numbers are not inherently equivalent to personal identification information.

Moreover, the Applicants respectfully submit that the cited passage fails to teach or suggest controlling user identification depending on each of the plurality of encryption keys as is required by claim 4.

For at least these reasons, the Applicants respectfully submit that claim 4 is not obvious over Matsuzaki in view of Johnson and further in view of Jackson and earnestly solicit allowance of the claim.

Claim 5

Claim 5 recites, in part, "an encryption circuit for encrypting desired data by use of a first encryption key and for encrypting the first encryption key and personal identification information by use of a second encryption key created out of a given piece of the personal identification information." Thus, claim 5 requires encrypting personal identification information by use of a second encryption key. Furthermore, it is evident from antecedent basis that the personal

identification information which is encrypted is the same personal identification information of which a given piece was used to create the second encryption key.

The Examiner alleges that paragraphs [0141], [0147], [0148] and [0152] of Matzusaki teach an encryption circuit for encrypting desired data by use of a first encryption key and for encrypting the first encryption key and personal identification information by use of a second encryption key. OA, pg. 5. After careful review of Matzusaki, the Applicants respectfully disagree with this interpretation.

The paragraph [0141] of Matsuzaki states:

> The encryption unit 102b, as the encryption unit 102, reads key information from the key storage medium 20, subjects the password received from the password input unit 101b to the encryption algorithm E1 using the read key information to generate an encrypted password, and writes the generated encrypted password as a file, to the storage unit 400b. Matsuzaki, para. [0141].

It is clear from this passage that the key information from the key storage medium and the password received from the password input unit are used to generate an encrypted password. By contrast, claim 5 requires encrypting personal identification information by use of an encryption key created out of a given piece of the personal identification information. Paragraph [0141] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The paragraphs [0147] and [0148] of Matsuzaki state:

> The encryption unit 203b, as the encryption unit 203, reads the plaintext file 401b from the storage unit 400b, and receives the file key from the file key generation unit 201b.
>
> The encryption unit 203b then subjects a plaintext included in the plaintext file 401b to the encryption algorithm E3 using the received file key as a key to generate a ciphertext, and writes an encrypted file 404b including the generated ciphertext in the data part thereof, to the storage unit 400. Matsuzaki, para. [0147]-[0148].

It is clear from this passage that the plaintext read from the storage unit and the file key received from the file key storage unit are used to generate a ciphertext. However, paragraphs [0147] and [0148] make no mention of encrypting personal identification information. The cited passage therefore clearly fails to teach the limitation of claim 5 requiring encrypting personal identification information by use of an encryption key created out of a given piece of the personal identification information.

The paragraph [0152] of Matsuzaki states:

> The encryption unit 204b reads the key information from the key storage medium 20, receives the file key from the file key generation unit 201b. The encryption unit 204b then subjects the file key to the encryption algorithm E4 using the read key information as a key to generate a second encrypted file key, and writes the generated second encrypted file key to the header part of the encrypted file 404b in the storage unit 400b. It should be noted here that the encryption algorithm E4 complies with DES. Matsuzaki, para. 0152.

The Applicants respectfully submit that paragraph [0152] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The Examiner further alleges that col. 10, ln. 48-65 of Johnson teaches creating an encryption key out of a given piece of personal identification information. OA, pg. 6. The cited passage is reproduced above in regards to claim 1. The Applicants submit that column 10, lines 48-65 of Johnson do not disclose encrypting personal identification information and creating a second encryption key out of a piece of the personal identification information. As previously noted, claim 5 requires that the personal identification information which is encrypted is the same as the personal identification information of which a given piece was used to create the second encryption key.

Additionally, the Examiner argues, "It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system." OA, pg. 6.

The Office Action, however has not explained, and it not evident, how employing the teachings of Johnson within the system of Matsuzaki enhances the security of the system. The Office Action has also not explained why a person of ordinary skill in the art would have found it obvious to reconstruct Matsuzaki to "enhance the security of the system." In this regard, neither Matsuzaki nor Johnson express any appreciation of such alleged advantages.

For at least these reasons, the Applicants respectfully submit that claim 5 is not obvious over Matsuzaki in view of Johnson and earnestly solicit allowance of the claim.

Claim 6

Claim 6 is dependent on and further limits claim 5. Since claim 5 is believed allowable, claim 6 is also believed allowable for at least the same reasons as claim 5.

Claim 10

Claim 10 is dependent on and further limits claim 7. Since claim 7 is believed allowable, claim 10 is also believed allowable for at least the same reasons as claim 7.

Claim 11

Claim 11 is dependent on claim 10 and recites, "The hard disk device according to claim 10, wherein the encryption function of the control mechanism creates a plurality of encryption keys out of a plurality of personal identification information and controls the user identification and the data encryption depending on each of the plurality of encryption keys, and the magnetic disk manages storage areas in accordance with the plurality of keys, and records the encrypted data in the respective storage areas by use of the corresponding encryption keys." It is emphasized that claim 11 requires the plurality of encryption keys to be created out of a plurality of personal identification information. Moreover, it is emphasized that claim 11 requires controlling user identification depending on each of the plurality of encryption keys.

The Examiner alleges that col. 8, ln. 33-47 of Jackson teach claim 4. OA, pg. 13. The Examiner argues that the cited claim elements are found in Jackson by merely copying the claim elements and

citing column and line numbers of Jackson in brackets. The rejection does not provide a comprehensive explanation of why the Examiner considers the limitations of claim 11 disclosed in Jackson. The Applicants are left guessing what the Examiner was thinking when making the rejection. If the rejection of claim 11 is maintained, the Applicants request that a detailed explanation of disclosed structures relied upon in Jackson be clearly articulated by the examiner in accordance with 37 CFR 1.104(c)(2).

The passage cited by the Examiner are recited above in regards to claim 4. The Applicants respectfully submit that the cited passage fails to teach or suggest a plurality of encryption keys which is created out of a plurality of personal identification information as required by claim 11 for the same reasons discussed above regarding claim 4. Moreover, the Applicants respectfully submit that the cited passage fails to teach or suggest controlling user identification depending on each of the plurality of encryption keys as is required by claim 11.

For at least these reasons, the Applicants respectfully submit that claim 11 is not obvious over Jackson in view of Johnson and earnestly solicit allowance of the claim.

Claim 12

Claim 12 is dependent on and further limits claim 7. Since claim 7 is believed allowable, claim 12 is also believed allowable for at least the same reasons as claim 7.

Claim 13

Claim 13 recites, in part, "wherein the data storage device includes an encryption function for encrypting desired data by use of a data encryption key and for encrypting personal identification information by use of a verification encryption key created out of a given piece of the personal identification information." Thus, claim 13 requires encrypting personal identification information by use of a verification encryption key. Furthermore, it is evident from antecedent basis that the personal identification information which is encrypted is the same personal identification information of which a given piece was used to create the verification encryption key.

The Examiner alleges that paragraphs [0141] and [0152] of Matsuzaki teach a data storage device including an encryption function for encrypting desired data by use of a data encryption key and for encrypting personal identification information by use of a verification encryption key. OA, pg. 6-7. After careful review of Matsuzaki, the Applicants respectfully disagree with this interpretation.The paragraph [0141] of Matsuzaki is recited above in regards to claim 1. It is clear from this passage that the key information from the key storage medium and the password received from the password input unit are used to generate an encrypted password. By contrast, claim 13 requires encrypting personal identification information by use of a verification encryption key created out of a given piece of the personal identification information. Paragraph [0141] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The paragraph [0152] of Matsuzaki is also recited above in regards to claim 1. The Applicants respectfully submit that paragraph [0152] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The Examiner further alleges that column 10, lines 48-65 of Johnson teaches creating an encryption key out of a given piece of personal identification information. OA, pg. 7. The cited passage is reproduced above in regards to claim 1. The Applicants submit that column 10, lines 48-65 of Johnson do not disclose encrypting personal identification information and creating a verification encryption key out of a piece of the personal identification information. As previously noted, claim 13 requires that the personal identification information which is encrypted is the same as the personal identification information of which a given piece was used to create the verification encryption key.

Additionally, the Examiner argues, “It would have been obvious to one having ordinary skill in the art at the time of applicant’s invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system.” OA, pg. 7. The Office Action, however has not explained, and it not evident, how employing the teachings of Johnson within the system of Matsuzaki

enhances the security of the system. The Office Action has also not explained why a person of ordinary skill in the art would have found it obvious to reconstruct Matsuzaki to "enhance the security of the system." In this regard, neither Matsuzaki nor Johnson express any appreciation of such alleged advantages.

For at least these reasons, the Applicants respectfully submit that claim 13 is not obvious over Matsuzaki in view of Johnson and earnestly solicit allowance of the claim.

Claim 14

Claim 14 is dependent on claim 13 and recites, "The information processing device according to claim 13, wherein the data encryption key and the verification encryption are mutually identical." It is evident from antecedent basis that the data encryption key and the verification encryption key recited in claim 14 are the same data encryption key and verification encryption key that were recited in claim 13.

Claim 14 is rejected under the same rationale as claim 13. OA, pg. 6-7. Thus, the reasons provided above as to why claim 13 is allowable apply equally to claim 14.

Additionally, in regards to claim 13, the Examiner alleges that "encrypting plaintext file using file key" teaches encrypting desired data by use of a data encryption key as required by claim 13. OA, pg. 6. The Examiner further alleges that "encrypting password using read key" teaches encrypting personal identification information by use of a verification encryption key as required by claim 13. OA, pg. 7. The "read key" refers to the read key information from the key storage medium, as the language "read key" is not used in any other context in paragraphs [0141] and [0152] of Matsuzaki. It follows from these statements that the Examiner is alleging the file key disclosed by Matsuzaki to be equivalent to the data encryption key of claim 13 and the read key of Matsuzaki to be equivalent to the verification encryption key of claim 13. It follows that Matsuzaki, alone or in combination with other teachings, cannot teach claim 14 unless the file key and the read key information are mutually identical.

The Applicants respectfully submit that Matsuzaki does not teach or suggest that the file key and the read key are mutually identical.

To the contrary, Matsuzaki discloses: "The file key generation unit 201b, as the file key generation unit 201, generates a file key, and outputs the generated file key to the encryption unit 202b, the encryption unit 203b, and the encryption unit 204b." Matsuzaki, paragraph [0143]. It is thus evident that the file key disclosed by Matsuzaki is generated by a file key generation unit. Matsuzaki additionally discloses, "The encryption unit 102b, as the encryption unit 102, reads key information from the key storage medium 20, subjects the password received from the password input unit 101b to the encryption algorithm E1 using the read key information to generate an encrypted password, and writes the generated encrypted password as a file, to the storage unit 400b." Matsuzaki, paragraph [0141]. It is thus evident that the read key information disclosed by Matsuzaki is read from a key storage medium. Furthermore, it is evident from fig. 10 of Matsuzaki that the file key generation unit (num. 201b) and the key storage medium (num. 20) are distinct. The fact that the file key and the read key information are generated or retrieved from distinct units suggests that the file key and the read key information are generally not mutually identical.

For at least these reasons, the Applicants respectfully submit that claim 14 is not obvious over Matsuzaki in view of Johnson and earnestly solicit allowance of the claim.

Claims 15-16

Claims 15 and 16 are dependent on and further limit claim 13. Since claim 13 is believed allowable, claims 15 and 16 are also believed allowable for at least the same reasons as claim 13.

Claim 17

Claim 17 recites, in part, "creating an encryption key out of a given piece of personal identification information; encrypting the personal identification information by use of the encryption key and thereby recording the encrypted personal identification information in the recording medium as verification data." Thus, claim 17 requires encrypting personal identification information by use of an encryption key. Furthermore, it is evident from antecedent basis that the personal identification information which is encrypted is the same

personal identification information of which a given piece was used to create the encryption key.

The Examiner alleges that paragraphs [0141] and [0152] of Matsuzaki teach encrypting personal identification information by use of an encryption key and thereby recording the encrypted personal identification information in the recording medium as verification data. OA, pg. 7. After careful review of Matsuzaki, the Applicants respectfully disagree with this interpretation.

The paragraph [0141] of Matsuzaki is recited above in regards to claim 1. It is clear from this passage that the key information from the key storage medium and the password received from the password input unit are used to generate an encrypted password. By contrast, claim 17 requires encrypting personal identification information by use of an encryption key created out of a given piece of the personal identification information. Paragraph [0141] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The paragraph [0152] of Matsuzaki is also recited above in regards to claim 1. The Applicants respectfully submit that paragraph [0152] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The Examiner further alleges that column 10, lines 48-65 of Johnson teach creating an encryption key out of a given piece of personal identification information. OA, pg. 8. The cited passage is reproduced above in regards to claim 1. The Applicants submit that column 10, lines 48-65 of Johnson do not disclose encrypting personal identification information and creating an encryption key out of a piece of the personal identification information. As previously noted, claim 17 requires that the personal identification information which is encrypted is the same as the personal identification information of which a given piece was used to create the encryption key.

Additionally, the Examiner argues, "It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system." OA, pg. 8.

The Office Action, however has not explained, and it not evident, how employing the teachings of Johnson within the system of Matsuzaki enhances the security of the system. The Office Action has also not explained why a person of ordinary skill in the art would have found it obvious to reconstruct Matsuzaki to "enhance the security of the system." In this regard, neither Matsuzaki nor Johnson express any appreciation of such alleged advantages.

For at least these reasons, the Applicants respectfully submit that claim 17 is not obvious over Matsuzaki in view of Johnson and earnestly solicit allowance of the claim.

Claim 18

Claim 18 is dependent on claim 17 and recites, in part, "encrypting the encryption key by use of a different encryption key and thereby recording the encrypted encryption key in the recording medium." It is evident from antecedent basis that the encryption key recited in claim 18 is the same encryption key that was recited in claim 17.

The Examiner alleges that paragraphs [0148] through [0152] of Matsuzaki teaches this limitation of claim 18. OA, pg. 10. The passage cited by the Examiner is reproduced above in regards to claim 2.

In regards to claim 17, the Examiner alleges that "encrypting password using read key and storing the encrypted password" teaches the limitation of claim 17 requiring encrypting personal identification information by use of an encryption key and thereby recording the encrypted personal identification information in the recording medium as verification data. OA, pg. 7. The "read key" refers to the read key information from the key storage medium, as the language "read key" is not used in any other context in paragraphs [0148] through [0152] of Matsuzaki. It follows from these statements that the Examiner is alleging the read key disclosed by Matsuzaki to be equivalent to the encryption key of claim 17. Furthermore, as previously noted, the encryption key of claim 18 is the same as the encryption key of claim 17. Therefore, Matsuzaki cannot teach claim 18 unless the read key information of Matsuzaki is equivalent to the encryption key of claim 18. It follows that Matsuzaki, alone or in combination with other

teachings, cannot teach claim 18 unless the read key information is encrypted by use of a different encryption key.

The Applicants respectfully submit that the cited passage of Matsuzaki fails to teach or suggest encrypting the read key information by use of a different encryption key. The passage teaches that a plaintext and a file key are encrypted. However, this fails to teach or suggest claim 18 because the plaintext and the file key are clearly not equivalent to the read key information.

For at least these reasons, the Applicants respectfully submit that claim 18 is not obvious over Matsuzaki in view of Johnson and earnestly solicit allowance of the claim.

Claim 19

Claim 19 recites, in part, "creating a verification encryption key out of a given piece of personal identification information; encrypting the personal identification information by use of the verification encryption key and recording the encrypted personal identification information in the recording medium as verification data, and further encrypting a data encryption key by use of the verification encryption key and thereby recording the encrypted data encryption key in the recording medium." Thus, claim 19 requires encrypting personal identification information by use of a verification encryption key. Furthermore, it is evident from antecedent basis that the personal identification information which is encrypted is the same personal identification information of which a given piece was used to create the verification encryption key.

The Examiner alleges that paragraphs [0141] and [0152] of Matsuzaki teach encrypting a personal identification information by use of a verification encryption key and recording the encrypted personal identification information in the recording medium as verification data. OA, pg. 8. After careful review of Matsuzaki, the Applicants respectfully disagree with this interpretation.

The paragraph [0141] of Matsuzaki is recited above in regards to claim 1. It is clear from this passage that the key information from the key storage medium and the password received from the password input unit are used to generate an encrypted password. By contrast, claim 19 requires encrypting personal identification information by use

of a verification encryption key created out of a given piece of the personal identification information. Paragraph [0141] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The paragraph [0152] of Matsuzaki is also recited above in regards to claim 1. The Applicants respectfully submit that paragraph [0152] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The Examiner further alleges that column 10, lines 48-65 of Johnson teaches creating an encryption key out of a given piece of personal identification information. OA, pg. 9. The cited passage is reproduced above in regards to claim 1. The Applicants submit that column 10, lines 48-65 of Johnson do not disclose encrypting personal identification information and creating a verification encryption key out of a piece of the personal identification information. As previously noted, claim 19 requires that the personal identification information which is encrypted is the same as the personal identification information of which a given piece was used to create the verification encryption key.

Additionally, the Examiner argues, "It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system." OA, pg. 9. The Office Action, however has not explained, and it not evident, how employing the teachings of Johnson within the system of Matsuzaki enhances the security of the system. The Office Action has also not explained why a person of ordinary skill in the art would have found it obvious to reconstruct Matsuzaki to "enhance the security of the system." In this regard, neither Matsuzaki nor Johnson express any appreciation of such alleged advantages.

For at least these reasons, the Applicants respectfully submit that claim 19 is not obvious over Matsuzaki in view of Johnson and earnestly solicit allowance of the claim.

Claim 20

Claim 20 is dependent on claim 19 and recites, "The data processing method for a data storage device according to claim 19, further comprising the step of: decrypting the encrypted data encryption key recorded in the recording medium along with a change in the personal identification information by use of the verification encryption key created out of the personal identification information prior to the change, and then encrypting the data encryption key again by use of the verification encryption key created out of the personal identification information after the change and thereby storing the data encryption key in the recording medium." It is evident from antecedent basis that the data encryption key, the verification encryption key and the personal identification information recited in claim 20 are the same data encryption key, verification encryption key and personal identification information that were recited in claim 19.

In regards to claim 19, the Examiner alleges that "the Examiner alleges that "encrypting password using read key and storing the encrypted password" teaches encrypting a personal identification information by use of a verification encryption key and recording the encrypted personal identification information in the recording medium as verification data. OA, pg. 8. The Examiner further alleges that "encrypting file key using read key" teaches encrypting a data encryption key by use of the verification encryption key. *Id.* The "read key" refers to the read key information from the key storage medium, as the language "read key" is not used in any other context in paragraphs [0141] and [0152] of Matsuzaki. It follows from these statements that the Examiner is alleging the file key of Matsuzaki to be equivalent to the data encryption key of claim 19, the read key of Matsuzaki to be equivalent to the verification encryption key of claim 19 and the password of Matsuzaki to be equivalent to the personal identification information of claim 19. Furthermore, as previously noted, it is evident from antecedent basis that the data encryption key, the verification encryption key and the personal identification information of claim 20 are the same as the corresponding elements of claim 19. Therefore, Matsuzaki cannot teach claim 20 unless the file key of Matsuzaki is equivalent to the data encryption key of claim 20, the read key information of Matsuzaki is equivalent to the verification

encryption key of claim 20 and the password of Matsuzaki is equivalent to the personal identification information of claim 20.

The Examiner alleges that paragraphs [0192] through [0199] of Matsuzaki teach claim 20. OA, pg. 10. After careful review of Matsuzaki, the Applicants respectfully disagree with this interpretation.

Paragraphs [0192] and [0193] of Matsuzaki state:

> (2) The following is an explanation of the operation of the file management apparatus 10b when a password is changed, with reference to a flowchart shown in FIG. 14.
>
> The password registration unit 100b reads key information from the key storage medium 20, reads a second encrypted file key from the encrypted file 404b, and subjects the second encrypted file key to the decryption algorithm D4 using the key information as a key to generate a file key (step S261). Following this, the password registration unit 100b receives an input of a new password from the user (step S262), subjects the generated file key to the encryption algorithm E2 using the new password as a key to generate a new first encrypted file key (step S263), and updates the first encrypted file key in the encrypted file 404b to the new first encrypted file key (step S264). Matsuzaki, para. [0192]-[0193].

The cited passage teaches that a file key is encrypted "using the new password as a key". However, the password disclosed by Matsuzaki is clearly not equivalent to the verification encryption key of claim 20. Therefore, the cited passage clearly fails to teach or suggest encrypting the data encryption key again by use of the verification encryption key created out of the personal identification information after the change as is required by claim 20.

Paragraph [0194] of Matsuzaki states:

> (4) The following is an explanation of the operation of the file management apparatus 10b when key information is updated, with reference to a flowchart shown in FIG. 15. Matsuzaki, para. [0194].

The Applicants respectfully submit that the cited passage clearly fails to teach or suggest encrypting the data encryption key again by use of the verification encryption key created out of the personal identification information after the change as is required by claim 20.

Paragraphs [0195] through [0197] of Matsuzaki state:

> (4) The following is an explanation of the operation of the file management apparatus 10b when key information is updated, with reference to a flowchart shown in FIG. 15.
>
> The key storage medium stores new key information beforehand, instead of the key information employed previously (referred to as old key information).
>
> The file encryption unit 200b receives an input of a password that is the same as the password received previously (step S281), reads a first encrypted file key from the encrypted file 404b (step S282), and subjects the first encrypted file key to the decryption algorithm D2 using the received password as a key to generate a file key (step S283). Following this, the file encryption unit 200b reads the new key information from the key storage medium, subjects the file key to the encryption algorithm E4 using the new key information as a key to generate a new second encrypted file key (step S284), and updates the second encrypted file key in the encrypted file 404b to the new second encrypted file key (step S285). Matsuzaki, para. [0195]-[0197] (emphasis added.)

The cited passage clearly teaches that the password is the same as the password received previously. As previously noted, Matsuzaki cannot teach claim 20 unless the password of Matsuzaki is equivalent to the personal identification information of claim 20. However, claim 20 requires a "verification encryption key created out of the personal identification information prior to the change" and further requires a "verification encryption key created out of the personal identification information after the change." It is clearly impossible to fulfill either requirement of claim 20 if no change to the personal identification information occurs.

Paragraphs [0198] and [0199] of Matsuzaki state:

> (5) In the above embodiment, the encrypted password is stored in a computer system in which a plaintext has been encrypted to generate a ciphertext, and so decryption of the ciphertext using a password is made only possible within the computer system. To enable the decryption of the ciphertext using the password in another computer system, the encrypted key may be stored in a portable storage medium, and inputted into the other computer system.
>
> Here, the password registration unit 100b in the computer system writes the encrypted password to a portable storage medium such as a SD memory card. Also, the user writes the encrypted file to

> another portable storage medium. The user then loads the portable storage medium to which the encrypted key has been written, and the portable storage medium to which the encrypted file has been written, on the other computer system, so that a file decryption unit in the other computer system reads the encrypted key from the portable storage medium, decrypts the read encrypted key, and also, reads the encrypted file from the portable storage medium, and decrypts the read encrypted file. Matsuzaki, para. [0198]-[0199].

The Applicants respectfully submit that the cited passage clearly fails to teach or suggest encrypting the data encryption key again by use of the verification encryption key created out of the personal identification information after the change as is required by claim 20.

For at least these reasons, the Applicants respectfully submit that claim 20 is not obvious over Matsuzaki in view of Johnson and earnestly solicit allowance of the claim.

Claim 21

Claim 21 is dependent on claim 19 and recites, "The data processing method for a data storage device according to claim 19, further comprising the step of: decrypting the encrypted data encryption key recorded in the recording medium upon disabling encryption of the data recorded in the recording medium by use of the verification encryption key created out of the personal identification information prior to a change and thereby storing the decrypted data encryption key in the recording medium." It is emphasized that claim 21 requires storing a decrypted data encryption key in a recording medium.

The Examiner alleges that para. 0192-0199 of Matsuzaki teaches claim 21. OA, pg. 10-11. Para. 0192-0199 of Matsuzaki are recited above in regards to claim 20.

The Applicants respectfully submit that the passage cited by the Examiner fails to teach or suggest storing a decrypted encryption key in a recording medium as is required by claim 21. To the contrary, the cited passage appears to teach encrypting the recorded encryption key in all cases where an encryption key is recorded in a recording medium.

For at least these reasons, the Applicants respectfully submit that claim 21 is not obvious over Matsuzaki in view of Johnson and earnestly solicit allowance of the claim.

Claim 22

Claim 22 is rejected under the same rationale as claim 17. OA, pg. 7-8. Thus, claim 22 is believed allowable for at least the reasons provided above regarding claim 17. The Applicants therefore respectfully submit that claim 22 is not obvious over Matsuzaki in view of Johnson and earnestly solicit allowance of the claim.

Claim 23

Claim 23 is rejected under the same rationale as claim 19. OA, pg. 8-9. Thus, claim 23 is believed allowable for at least the reasons provided above regarding claim 19. The Applicants therefore respectfully submit that claim 23 is not obvious over Matsuzaki in view of Johnson and earnestly solicit allowance of the claim.

CONCLUSION

In view of the forgoing remarks, it is respectfully submitted that this case is now in condition for allowance and such action is respectfully requested. If any points remain at issue that the Examiner feels could best be resolved by a telephone interview, the Examiner is urged to contact the attorney below.

No fee is believed due with this Amendment, however, should such a fee be required please charge Deposit Account 50-0510 the required fee. Should any extensions of time be required, please consider this a petition thereof and charge Deposit Account 50-0510 the required fee.

Respectfully submitted,

Dated: October 8, 2007

/ido tuchman/

Ido Tuchman, Reg. No. 45,924
Law Office of Ido Tuchman
82-70 Beverly Road
Kew Gardens, NY 11415
Telephone (718) 544-1110
Facsimile (866) 607-8538